5. *Титов С. С., Торгашова А. В.* Генерация неприводимых многочленов, связанных степенной зависимостью корней // Докл. Том. гос. ун-та систем управления и радиоэлектроники. Томск : ТУСУР, 2010. Вып. № 2 (22), ч. 1. С. 310–318.

ПОСТРОЕНИЕ НЕПРИВОДИМЫХ МНОГОЧЛЕНОВ ПРОСТЫХ ПОРЯДКОВ

Кр. Л. Геут, С. С. Титов
(Екатеринбург, УрГУПС, gluskokrl@rtural.ru)

Неприводимые многочлены нашли свое применение в различных областях математики, информационной техники и защите информации. Неприводимым называется многочлен с коэффициентами из $GF(q)$ (т. е. многочлен над конечным полем $GF(q)$), не являющийся произведением двух многочленов меньшей ненулевой степени.

Неприводимые многочлены, с помощью которых фактически строятся поля Галуа, являются аналогом простых чисел в натуральном ряду. Нахождение их, как и простых чисел, производится подбором и требует больших затрат вычислительных мощностей сверхбыстродействующих ЭВМ. Использование свойств неприводимых многочленов позволяет максимизировать эффективную компьютерную реализацию арифметики в конечных полях, что имеет особое значение для криптографии и теории кодирования. Так, например, реализация электронной цифровой подписи на эллиптических кривых в полях большой степени является актуальной задачей электронной коммерции.

Среди неприводимых многочленов особый интерес представляют примитивные многочлены, т. е. такие, корни которых являются примитивными (или порождающими) элементами поля разложения этого многочлена. Примитивные элементы являются основаниями дискретных логарифмов, находящих широкое применение в асимметричной криптографии [1; 2].

Однако в некоторых случаях для решения конкретных задач необходимо построить неприводимый многочлен заданных параметров. Многочлены конечных полей характеристики два используются для описания регистров сдвига, которые являются основным устройством работы большинства технических устройств шифрования в криптографии. Так, к примеру, для программирования конечного автомата цикла $\operatorname{ord} f \neq 2^n - 1$ необходим непримитивный многочлен степени n.

Пусть p – простое число, и пусть $g_{p-1}(x)$ разлагается в произведение симметричных многочленов степени $2k$; тогда имеем $g_{p-1}(x)$ делит g_2^k, т. е. $2^k + 1 \equiv 0 \pmod p$, т. к. $p = \operatorname{ord} f$ для $f(x)$, делящего $g_{p-1}(x)$.

Обратно, пусть p – простое число, k – наименьшее такое, что $2^k \equiv -1 \pmod p$. Тогда $g_{p-1}(x)$ делит g_2^k (и такая степень двойки в индексе – наименьшая возможная), отсюда $g_{p-1}(x)$ разлагается в произведение неприводимых симметричных многочленов степеней $2m$, где k/m нечетно, отсюда $k = m$, т. к. ясно, что если p – простое число и $g_{p-1}(x)$ разлагается в произведение неприводимых многочленов $q_j(x)$ $(j \geq 1)$ одной и той же степени. Пусть $\deg f = n$, $\operatorname{ord} f = p$, $f(x)$ неприводим, тогда $|< x >| = p$ в $K_f \approx GF(2^n)$, и для любого $y \neq 1$, $y \in < x >$ имеем $< y > = < x >$ (т. к. p – простое число); следовательно, никакой $y \neq 1$, $y \in < x >$ не принадлежит собственному подполю поля $GF(2^n) \approx K_f$, т. е. y удовлетворяет неприводимому уравнению той же степени n [2; 3].

Степень таких неприводмых многочленов определяется как наименьшая натуральная степень n такая, что $2^n = 1 \pmod p$. Соответственно их количество $j = \dfrac{p-1}{n}$. В случае если неприводимых многочленов $q_j(x)$ $(j \geq 1)$ искомого порядка два, то их поиск сводится к нахождению наибольшего общего делителя многочленов $s(x) = \sum_{i=1}^{n} 2^i \bmod p$ и $t(x) = \sum_{i=0}^{p-1} x^i \Leftrightarrow t(x) = \sum_{i=1}^{p} x^i$ (выбор формулы зависит от значения следа многочлена $q_j(x)$). Если же таких многочленов $q_j(x) > 2$, то задача сложнее, т. к. НОД в таком случае будет произведением всех $q_j(x)$ с заданным значением следа $Tr(x) = \{0, 1\}$ [4].

Пример 1. Рассмотрим $\operatorname{ord} f = 43$.

Решаем уравнение $2^n = 1 \pmod{43}$, $n = \deg f = 14$, $(43 - 1)/3 = 14$, т. е. 3 неприводимых многочлена порядка $\operatorname{ord} f = 43$ и степени $\deg f = 14$.

Найдем $u(x) = \text{НОД}\,[t(x) = \sum_{i=1}^{43} x^i\,] = \text{НОД}\,[x^{43} + x^{42} + x^{41} + x^{40} +$

$+ x^{39} + x^{38} + x^{37} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} +$

$+ x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} +$

$+ x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x;\ x^{42} + x^{41} + x^{39} + x^{35} +$

$+ x^{32} + x^{27} + x^{22} + x^{21} + x^{16} + x^{11} + x^8 + x^4 + x^2 + x] = x^{28} + x^{26} + x^{25} + x^{20} +$

$+ x^{19} + x^{18} + x^{14} + x^{10} + x^9 + x^8 + x^3 + x^2 + 1.$

Многочлен $x^{28} + x^{26} + x^{25} + x^{20} + x^{19} + x^{18} + x^{14} + x^{10} + x^9 + x^8 + x^3 +$ $+ x^2 + 1$ является произведением $q_1(x)q_2(x)$ со значениями следа $Tr(x) = 0$. А третий многочлен $q_3(x)$ можно получить, разделив $t(x)$ на $u(x)$, т. е. $\dfrac{t(x)}{q_1(x)q_2(x)} = q_3(x) = x^{14} + x^{13} + x^{11} + x^7 + x^3 + x + 1$, $Tr(x) = 1$. Для вычисления $q_1(x)$ и $q_2(x)$ воспользуемся теоремой Виета: $u(x) = (x^{14} + \sigma_1 x^{13} + \sigma_2 x^{12} + \sigma_3 x^{11} + \ldots + \sigma_{13} x + 1)$, где $\sigma_1 =$

$= \sum_{i=1}^{14} 2^i \bmod 43$, $\sigma_2 = \sum_{i \neq j} 2^i 2^j \bmod 43$, $\sigma_3 = \sum_{i \neq j \neq k} 2^i 2^j 2^k \bmod 43$ и т. д.

В данном примере достаточно вычислить σ_1.

После необходимых расчетов получаем многочлен $v(x) = x^{42} +$ $+ x^{41} + x^{40} + x^{39} + x^{38} + x^{37} + x^{35} + x^{33} + x^{32} + x^{31} + x^{27} + x^{24} + x^{23} + x^{22} + x^{21} +$ $+ x^{20} + x^{19} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$

$q_1(x) = \text{НОД}\,[v(x), u(x)] = x^{14} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 +$ $+ x^3 + 1.$

$q_2(x) = u(x) / q_1(x) = x^{14} + x^{12} + x^{10} + x^7 + x^4 + x^2 + 1.$

Еще одним примером использования неприводимых многочленов над конечными полями являются гауссовы нормальные базисы [1; 2]. Рассмотрим конечные поля нечетной характеристики. ГНБ

в поле $GF(q^n)$ порождается элементом $x = \alpha = \zeta + \zeta^{\gamma} + \zeta^{\gamma^2} + \ldots + \zeta^{\gamma^{k-1}}$, где $p = kn + 1$ – простое число (т. н. базис k-го типа);

ζ – корень p-й степени из единицы в поле $GF(q^{kn})$ (очевидно, примитивный при $\zeta \neq 1$ ввиду простоты числа p), т. е. $\zeta^p = 1$, причем $GF(q^n) \subset GF(q^{kn})$.

γ – примитивный корень k-й степени из единицы в поле Z_p вычетов по модулю p, причем γ вместе с q порождают всю (мультипликативную) группу Z_p^* ненулевых вычетов по модулю p.

Нормальный базис $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ [5], $\zeta^{p-1} + \zeta^{p-2} + \ldots + \zeta + 1 = 0$.

При этом необходимым и достаточным условием существования ГНБ k-го типа, кроме простоты числа $p = kn + 1$, не делящего q, является взаимная простота чисел n и kn/d, где d – порядок подгруппы, порожденный числом q в группе Z_p^*. В частности, это выполняется при $d = kn$ (т. е. если q – первообразный по модулю p).

Пример 2. При $q = 3$, $p = 5$, $k = n = 2$, $d = 2 \times 2 = 4$, т. к. $3^1 = 3$, $3^2 = 9 = 4 \pmod 5$, $3^3 = 27 = 2 \pmod 5$, $3^4 = 81 = 1 \pmod 5$, т. е. $q = 3$ – первообразный корень по модулю 5. $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$, $\zeta^5 = 1$, $\gamma = 4$, т. к. в группе $Z_5^* = \{1, 2, 3, 4\}$ только $\gamma = 4$ удовлетворяет условию $\gamma^k = \gamma^2 = 1$, $\gamma \neq 1$. Имеем $\zeta \in GF(3^4)$, т. к. $F(z) = z^4 + z^3 + z^2 + z + 1$ неприводим над $GF(3)$. Для проверки необходимо перебрать все возможные корни из поля $GF(3)$:

$F(0) = 0^4 + 0^3 + 0^2 + 0 + 1 = 1 \neq 0$;

$F(1) = 1^4 + 1^3 + 1^2 + 1 + 1 = 1 \pmod 3 \neq 0$;

$F(2) = 2^4 + 2^3 + 2^2 + 2 + 1 = (-1)^4 + (-1)^3 + (-1)^2 + (-1) + 1 = 1 \neq 0$.

Мы строим $x = \alpha = \zeta + \zeta^4 = \zeta + \zeta^{-1}$, $x^q = x^3 = \alpha^3 = \zeta^3 + \zeta^{-3} = \zeta^3 + \zeta^2$, так что $\{\alpha, \alpha^3\}$ должен быть нормальным базисом в $GF(3^2)$. Каков характеристический многочлен $f(x)$ для $x = \alpha$?

Вычисляем:

$x^2 = \zeta^2 + 2\zeta\zeta^{-1} + \zeta^{-2} = \zeta^2 + 2 + \zeta^3$, поэтому $x^2 + x = \zeta + \zeta^2 + \zeta^3 + \zeta^4 + 2 = (\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1) + 1 = 0 + 1 = 1$, так что x удовлетворяет уравнению $x^2 + x = 1$, т. е. $x = \alpha$ есть корень многочлена

$f(x) = x^2 + x - 1$, т. е. x – корень многочлена $f(x) = x^2 + x + 2$, который должен быть неприводимым над $GF(3)$:

$f(0) = 0^2 + 0 + 2 = 2 \neq 0$;

$f(1) = 1^2 + 1 + 2 = 1 \pmod 3 \neq 0$;

$f(2) = 2^2 + 2 + 2 = (-1)^2 + (-1) + 2 = 2 \neq 0$.

При этом $\alpha^4 = \alpha\alpha^3 = \zeta^4 + \zeta^{-2} + \zeta^2 + \zeta^{-4} = \zeta^1 + \zeta^2 + \zeta^3 + \zeta^4 = -1$, т. е. α – примитивный, причем $\alpha^8 = \alpha^{3^{\wedge}2-1} = (-1)^2 = 1$.

Пример 3. При $q = 3$, $p = 17$, $k = n = 4$, многочлен $F(z) = z^{16} + z^{15} + \ldots + z + 1$ неприводим над $GF(3)$, т. к. тройка – первообразный корень по модулю $p = 17$, и если $F(\zeta) = 0$, то $\zeta^{17} = 1$. Уравнение $\gamma^k = 1$, т. е. $\gamma^4 = 1$, имеем в $Z_p = Z_{17}$ следующие корни: во-первых, поскольку $2^4 = 16 \equiv -1 \pmod{17}$, имеем $(2^4)^2 = (2^2)^4 \equiv +1 \pmod{17}$, поэтому $\gamma = \gamma_1 = 4$; далее, $\gamma_2 = \gamma_1^2 = 16 \equiv -1 \pmod{17}$, $\gamma_3 = \gamma_1^3 = -4 \equiv 13 \pmod{17}$ и, наконец, $\gamma_4 = \gamma_0 = \gamma_1^4 = 1$. Так что можно взять за примитивный корень четвертой степени из единицы $\gamma = 4$ и получить $x = \alpha = \zeta + \zeta^{\gamma} + \zeta^{\gamma^{\wedge}2} + \zeta^{\gamma^{\wedge}3} = \zeta^{\gamma 1} + \zeta^{\gamma 2} + \zeta^{\gamma 3} + \zeta^{\gamma 4} = \zeta + \zeta^4 + \zeta^{-1} + \zeta^{4}$, при этом множество $\{\alpha, \alpha^3, \alpha^9, \alpha^{27}\}$ должно быть нормальным базисом в $GF(q^n) = GF(3^4)$. Каков характеристический многочлен $f(x)$ для $x = \alpha$?

Вычисляем: учитывая, что $\zeta^{17} = 1$.

$\alpha = \zeta^1 + \zeta^4 + \zeta^{-4} + \zeta^{-1}$;

$\alpha^3 = \zeta^3 + \zeta^{12} + \zeta^{-12} + \zeta^{-3} = \zeta^3 + \zeta^5 + \zeta^{-5} + \zeta^{-3}$;

$\alpha^9 = \zeta^9 + \zeta^{15} + \zeta^{-15} + \zeta^{-9} = \zeta^2 + \zeta^9 + \zeta^{-9} + \zeta^{-2} = \zeta^8 + \zeta^2 + \zeta^{-2} + \zeta^{-8}$;

$\alpha^{27} = \zeta^6 + \zeta^{24} + \zeta^{-24} + \zeta^{-6} = \zeta^6 + \zeta^7 + \zeta^{-7} + \zeta^{-6}$.

Видим, что:

$\sigma_1 = Tr\,\alpha = \alpha + \alpha^3 + \alpha^9 + \alpha^{27} = \zeta^1 + \zeta^2 + \ldots + \zeta^8 + \zeta^{-8} + \ldots + \zeta^{-2} + \zeta^{-1} = \zeta^{16} + \zeta^{15} + \ldots + \zeta^2 + \zeta = -1 \equiv 2 \pmod 3$, так что, поскольку $f(x) = x^4 - \sigma_1 x^3 + \sigma_2 x^2 - \sigma_3 x + \sigma_4$, получаем: $f(x) = x^4 - (-1)\,x^3 + \ldots = x^4 + x^3 + \ldots$, теперь надо найти остальные коэффициенты.

Вычисляем: $\alpha^4 = \alpha \times \alpha^3 = \zeta^4 + \zeta^6 + \zeta^{-4} + \zeta^{-2} + \zeta^7 + \zeta^9 + \zeta^{-1} + \zeta^1 + \zeta^{-1} + \zeta^1 + \zeta^{-9} + \zeta^{-7} + \zeta^2 + \zeta^4 + \zeta^{-6} + \zeta^{-4} = 2\zeta^1 + \zeta^2 + 2\zeta^4 + \zeta^6 + \zeta^7 + \zeta^8 + \zeta^{-8} + \zeta^{-7} + \zeta^{-6} + 2\zeta^{-4} + \zeta^{-2} + 2\zeta^{-1} \neq 1$ (т. к. $\zeta^9 = \zeta^{-8}$).

Вычисляем: $\alpha^2 = \alpha \times \alpha = \zeta^2 + \zeta^8 + \zeta^{-8} + \zeta^{-2} + 2\zeta^5 + 2\zeta^{-3} + 2 + 2 + 2\zeta^3 + 2\zeta^{5} = 1 + \zeta^2 + 2\zeta^3 + 2\zeta^5 + \zeta^8 + \zeta^{-8} + 2\zeta^{-5} + 2\zeta^{-3} + \zeta^{-2}$.

$\sigma_4 = \alpha\alpha^3\alpha^9\alpha^{27} = \alpha^4\alpha^{36} = \alpha^4(\alpha^4)^9 = \alpha^{40} = (\alpha^8)^5$.

$(\alpha^4)^9 = 2\zeta^9 + \zeta^{18} + 2\zeta^{36} + \zeta^{54} + \zeta^{63} + \zeta^{72} + \zeta^{-72} + \ldots = 2\zeta^9 + \zeta^1 + 2\zeta^2 + \zeta^3 + \zeta^{12} + \zeta^4 + \zeta^{4} + \ldots = \zeta^1 + 2\zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + 2\zeta^8 + 2\zeta^{-8} + \ldots$

$\sigma_2 = \alpha^4 + \alpha^{10} + \alpha^{28} + \alpha^{12} + \alpha^{30} + \alpha^{36}$.

$\alpha^{10} = \alpha\alpha^9 = \zeta^9 + \zeta^3 + \zeta^{-1} + \zeta^{-7} + \zeta^{12} + \zeta^6 + \zeta^2 + \zeta^{4} + \zeta^4 + \zeta^{-2} + \zeta^{-6} + \zeta^{-12} + \zeta^7 + \zeta^1 + \zeta^{-3} + \zeta^{-9} = \zeta^1 + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^8 + \zeta^{-8} + \ldots = -1$, значит, $\alpha^{40} = 1$, $\sigma_4 = 1$, $\alpha^5 \neq 1$, α – не примитивен.

Отсюда: $\alpha^{30} = (-1)^3 = -1 \equiv 2 \pmod 3$,

$\alpha^{20} = (-1)^2 = 1 = 2\zeta^1 + \ldots + 2\zeta^{16}$.

Вычисляем: $\alpha^4 + \alpha^3 + 1 = 2\zeta^1 + \zeta^2 + \zeta^3 + 2\zeta^4 + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^8 + \zeta^{-8} + \ldots + 2\zeta^1 + \ldots + 2\zeta^{-1} = \zeta^1 + \zeta^4 + 0 + \zeta^{-4} + \zeta^{-1}$.

Заменяя 1 на сумму $2\zeta^1 + \ldots + 2\zeta^{16} = 2\zeta_1^{1} + \ldots + 2\zeta^8 + 2\zeta^{-8} + \ldots + 2\zeta^{-1}$, получим $\alpha^2 = 2\zeta^1 + \zeta^3 + 2\zeta^4 + \zeta^5 + 2\zeta^6 + 2\zeta^7 + 2\zeta^{-7} + \ldots = 2\alpha + \alpha^3 + 2(\zeta^6 + \zeta^{-6}) + 2(\zeta^7 + \zeta^{-7})$.

$\alpha^4 + \alpha^3 = 2\zeta^1 + \zeta^2 + \zeta^3 + 2\zeta^4 + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^8 + \zeta^{-8} + \ldots$

Видим, что: $\alpha^4 + \alpha^3 + 1 = \zeta^1 + \zeta^4 + \zeta^{-4} + \zeta^{-1} = \alpha^1$, т. к. $1 = 2\zeta^1 + \ldots + 2\zeta^{16}$, т. е. $\alpha^4 + \alpha^3 - \alpha + 1 = 0$ (α^2 не нужен). Значит, α есть корень x неприводимого над $GF(3)$ многочлена $f(x) = x^4 + x^3 - x + 1$. Его порядок равен порядку α и равен 20, т. к. $\alpha^{10} = -1 \neq 1$ и $\alpha^4 \neq 1$.

При этом $\beta = \alpha^4$ имеет порядок 5, т. к. $\beta^5 = (\alpha^4)^5 = \alpha^{20} = 1$, и удовлетворяет уравнению $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$. Порядок корня σ неприводимого над $GF(3)$ многочлена степени n имеет порядок, делящий $3^n - 1$. $3^1 - 1 = 3 - 1 = 2 \neq 0 \pmod 5$, $3^2 - 1 = 9 - 1 = 8 \neq 0 \pmod 5$, $3^3 - 1 = 26 \neq 0 \pmod 5$, $3^4 - 1 = 80 \neq 0 \pmod 5$).

Неприводимость β равносильна первообразности тройки.

Итак, в работе рассмотрены алгоритмы генерации неприводимых многочленов данного простого порядком в конечных полях различных характеристик, что позволяет решать конкретные задачи в области шифрования, криптографии и других областях защи-

ты информации. В дальнейшем планируется продолжить расчеты многочленов больших степеней.

Библиографические ссылки

1. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М. : МЦНМО, 2004. 470 с.

2. *Лидл Р., Нидеррайтер Г.* Конечные поля : в 2 т. / пер. с англ. М. : Мир, 1988. Т. 1. 430 с.

3. *Демкина О. Е., Титов С. С., Торгашова А. В.* Рекуррентное вычисление неприводимых многочленов в задачах двоичного кодирования // Молодые ученые – транспорту : тр. IV науч.-техн. конф. Екатеринбург: УрГУПС, 2003. С. 391–404.

4. *Баданова О. М., Ициксон М. А., Титов С. С., Усольцев А. В.* Вычисление коэффициентов неприводимых делителей суммы геометрической прогрессии // Проблемы теоретической и прикладной математики : тр. 34-й регион. молодежной конф. Екатеринбург : УрО РАН, 2003. С. 3–4.

5. *Глуско К. Л., Титов С. С.* Арифметический алгоритм решения квадратных уравнений в конечных полях характеристики два // Докл. Том. гос. ун-та систем управления и радиоэлектроники. Томск : ТУСУР, 2012. № 1(25), ч. 2. С. 148–152.

АСИММЕТРИЧНЫЙ АЛГОРИТМ ШИФРОВАНИЯ

Н. Н. Гладков, М. А. Балашов, Т. Е. Иванов, С. С. Титов
(Екатеринбург, УрГУПС)

В наше время актуальной проблемой информационной безопасности является обеспечение безопасного обмена информацией между двумя пользователями. Одним из решений этой проблемы является использование алгоритмов шифрования, более надежными из которых являются асимметричные алгоритмы.

Асимметричный алгоритм шифрования – это алгоритм, использующий два математически связанных шифровальных ключа. Один ключ называется секретным и хранится в недоступном месте.